OFF-LINE PIN VERIFICATION USING IDENTITY-BASED SIGNATURES

W. Dale Hopkins

ABSTRACT

A method for off-line Personal Identification Number (PIN) verification using a smart card accessed on an off-line terminal comprises creating a unique secret key for an enrolled smart card using a card issuer private key, and generating signatures on an entered PIN using the unique key. The signatures are verifiable by the smart card and/or the terminal.